

C I A C

Computer Incident Advisory Capability

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information

CIAC-2307 R.1

by Richard Feingold

February, 1995



DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This report has been reproduced
directly from the best available copy.

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (615) 576-8401, FTS 626-8401.

Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.
Springfield, VA 22161

CIAC is the U.S. Department of Energy's Computer Incident Advisory Capability. Established in 1989, shortly after the Internet Worm, CIAC provides various computer security services free of charge to employees and contractors of the DOE, such as:

- Incident Handling consulting
- Computer Security Information
- On-site Workshops

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.

This is an informal report intended primarily for internal or limited external distribution. The opinions and conclusions stated are those of the author and may or may not be those of the Laboratory.

Work performed under the auspices of the U. S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Table of Contents

Abstract	1
Introduction	1
The Threats	2
Resources and Counter-measures	4
Electronic Mail	6
Anonymous ftp	7
Electronic Bulletin Board Services.....	9
Electronic Conferencing	9
List Servers/ Information Sources.....	10
Network Information	10
Reference Services	11
USEnet News	12
The DOE Automated Departmental Directives System (ADDS)	13
The National Institute of Standards and Technology (NIST) Electronic Bulletin Board Services	13
The DOE Computer Incident Advisory Capability (CIAC) File Server and Electronic Bulletin Board System	13
The National Computer Security Center (NCSC).....	14

Table of Contents, Continued

Appendix A	
Glossary and Notation	A-1
Appendix B	
Anonymous ftp Sites	B-1
Appendix C	
Finger Sources	C-1
Appendix D	
BBSs	D-1
Appendix E	
IRC (Internet Relay Chat) Conferencing	E-1
Appendix F	
List Servers/Information Sources	F-1
Appendix G	
Network Information	G-1
Appendix H	
Reference Services	H-1
Appendix I	
Remailers	I-1
Appendix J	
USEnet News	J-1
Appendix K	
FIRST	K-1
Appendix L	
References	L-1
Appendix M	
Contacting CIAC	M-1

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information

Abstract

The quantity, quality, and availability of electronic resources is multiplying rapidly. Information Technology (IT) security professionals must make timely and effective use of these resources if they are to contain the growing threats of globally networked attackers. This paper outlines the threats, including recent examples, and then provides multi-level descriptions of the abundant resources available to the information technology security community. These descriptions are valuable to everyone from networking novices to sophisticated experts. While the information is useful for the entire security community, this paper pays particular attention to Department of Energy requirements.

Introduction

Information Technology (IT) security professionals are battling network attackers. Each of the professionals—from the operations level down to the assistant computer security officer, whether classified or unclassified, manager or user—must maintain their ability to recognize the threat and acquire the appropriate countermeasures. They must gain and maintain knowledge and ability to use the ever increasing resources—on parity with the attackers. This paper opens the door for the novice and enlarges the opening for the expert. It increases the reader's threat awareness and enables effective and efficient use of the resources that attackers will certainly use against us. In short, cognizance of electronic resources is critical—they are the common ground of both information technology threats and countermeasures. The attackers use the resources with abundant facility; we must become at least as proficient. The remainder of this section sets the perspective of the exposition that follows.

Over two decades ago, the futurist Marshall McLuan made the observation that “the electronic interconnections will make the Earth a global village.” It was a brilliant metaphor and qualitatively predicted the electronic way of life for many of us. What is far more problematic is the quantitative impact of the electronic interconnections on what we as computer security professionals do—specifically, ensuring secure networking and computation for our constituents.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

The network¹ is the product of a rapidly developing technology and the need to interconnect information resources. As a recent phenomenon without historical precedence and paradigm, it raises new challenges to our abilities to manage vast resources. Often, the incremental cost of obtaining valuable information is insignificant. A document available on the network is an inexhaustible supply of its own copies. Most users are not only in instantaneous contact with each other, but with each other's private and public databases and other online information.

It is an estimated² that there are over three million nodes on the Internet—the network of networks that links a significant portion of the Earth's intellectual community. Each machine on the Internet has between one and many thousands of users and these machines are found just about anywhere on the planet. In principle, any user on any node can access or transfer information to or from any other node, use its resources, and even log in to it.³

To the novice, this myriad of actual and potential connections, this diversity of protocols, this spectrum of philosophies is an incomprehensible maze. Remarkably, with a little training and a modest amount of determination bolstered by need, the electronic world opens a new facility in communications as well as a vast store of information. To obtain a true perspective of its expanse and appreciation of its capabilities, one must *experience* the network.

The Threats

The average computer attacker⁴ is no more a technological genius than the average driver is a brilliant automotive engineer. The danger is not so much his⁵ native intelligence as his acquired knowledge, training, and facility with the network structures. Notwithstanding the legal, moral, ethical, and pragmatic issues, trying to reduce the free flow of questionable information on the network would be unmanageable at best; trying to eliminate it would be unimaginable. Our goal as security professionals is to recognize and understand of threats.

Attackers gain both qualitative and quantitative advantages from their facility with the network. Qualitatively, they have access to extremely effective communications channels. The Internet Relay Chat (IRC) allows them to anonymously and openly discuss whatever they want at minimal (if any) cost, while simultaneously being able to surreptitiously exchange private correspondences of any kind. For example, someone creates an accurate and instantly updatable index of online cracking tools and then posts it on the network, making it and unlimited copies immediately available to the global cracking community.

¹ The network for the purpose of this discussion is a generic term signifying the many methods of electronic interconnections. The conceptual domain is sometimes referred to as "*cyberspace*."

² Recent estimates by reliable sources; there is no way to know for certain.

³ In practice, of course, many of the nodes have some degree of security which prohibits some or all levels of arbitrary access.

⁴ This document's term for an electronic criminal; other, possibly more ambiguous terms are *hacker*, *intruder*, *cyberpunk*, *phreak*, and so on.

⁵ The masculine pronoun with neutral intent is used for rhetorical smoothness. I find *s/he*, *his/her*, *his* or *her* awkward and distracting.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

This also highlights the quantitative aspect of the attacker advantage. The amount of time individuals save by immediately taking advantage of each other's efforts is immeasurable. They often use free⁶ resources and appear to have abundant personal time. Attackers frequently use personal computers as well as computer accounts on obliging or compromised systems to search the network for vulnerabilities.

Examples

Early in 1994, the Internet experienced a continuing series of "sniffer" attacks. That is, attackers compromised host systems, installed software that monitored and recorded specific Local Area Network transactions that included host name/user name/password combinations. Some intruders evaded detection through the use of sophisticated Trojan software. It only took a one or a few talented individuals to create the software and techniques that were then used by many to compromise at the least hundreds of thousands⁷ of accounts.

A full-time physicist and part-time computer security expert discovered a significant security vulnerability. It was in a popular operating system on a popular workstation. He wrote a program to exploit the vulnerability, complete with detailed comments, and submitted it to the vendor of the workstation as well as reliable computer security groups. The vendor responded and eventually created a patch to fix the vulnerability. Ironically, the program fell into attacker hands—we still do not know how—and is widely being used to exploit unpatched workstations. Evidently, the attackers can circulate the program quicker than the security community can disseminate the countermeasures.

⁶ Clearly any resource has a cost; chances are the crackers are not paying. When the marginal costs are so low, there is no economical way of recovering them at the user level—they are absorbed as institutional overhead.

⁷ CERT estimate.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

The Electronic Frontier Foundation⁸, a non-profit organization created to promote the free exchange of information on the network (among other things), provides a repository for “Computer Underground Digest” (CUD) publications. Literary merit notwithstanding, these (quasi) periodicals frequently contain significant attacker information, including detailed methodologies on defeating toll call controls (Phone Phreaking), a complete list of credit card prefixes, intimate information on computer and network vulnerabilities, and so on. To get a feel for the authors’ level of defiance and perversity, one publication has detailed and accurate instructions on the construction of a light bulb bomb; another on how to manufacture nitroglycerine. Recently, someone posted a comprehensive index to the CUD—a substantial time and labor saving compendium for attackers.

The IRC links attackers from everywhere; they can exchange information (figuratively) across the table or under the table—in real time. Recently, user name password pairs from newly compromised university computer systems were openly posted on the IRC channel #hack.

Resources and Counter- measures

We will discuss several major network resources; there are others in the references at the end of this document; and there are still others that may be discovered simply by browsing the network. At the introduction of each resource, we will offer suggestions of how the resource may be used to counter attackers and other possible adverse activities. Of course, any technology that makes you more efficient and effective will help achieve that goal.

There is no single expert on all network resources. There is no single up-to-date compendium. There is no single structure that governs or manages all resources. The network is both planned and unplanned—with formal, defacto, and sometimes incompatible standards. Its growth is both revolutionary and evolutionary. This document provides a high level view of a selected subset of resources and services, providing sufficient detail for the novice to get started and for most sophisticated users to learn something new.

⁸ The EFF provides an open, uncensored service with significant value to the general community as well as information security professionals.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

Electronic mail (E-mail) delivers messages between physically distant points, often within minutes. File transfer copies information at hundreds or thousands of characters per second.⁹ The USEnet news group service provides an open electronic exchange of information in thousands of special interest groups. The IRC provides conferencing where special interest groups meet electronically to “chat” and exchange information.¹⁰ Electronic Bulletin Board Services (BBS) are a relatively mature and stable method of information exchange. Electronic list servers provide moderated and unmoderated collection and dissemination of contributor supplied information on specific topics. There are electronic reference services that allow a user to hierarchically search the entire spectrum of network resources for specific subjects or services. Finally, there is a network information provider.

For information technology security specialists, discovering that attackers routinely exploit these network resources is the first step. Appreciating their strategic and tactical value is the next. The third step is learning how to use them. Experienced IT specialists, even those unfamiliar with Unix, TCP/IP, and/or the Internet, will find that the network is a timely and powerful strategic asset; a remarkably effective system of communication requiring their serious attention.

The following sections introduce each of the resources mentioned above¹¹ (E-mail first, the remainder in alphabetical order). The best and most effective way to learn is by doing. Examples and help texts for ftp and rn appear in the appendices. This is a rapidly emerging suite of resources, where good, up to date documentation is scarce. Even the online documentation tends to age quickly—and is usually only updated as an afterthought.

⁹ The proposed National Information Infrastructure (NII) calls for transfer rates of gigabits/second.

¹⁰ The conceptual location of the “chat,” since it is physically distributed among terminals and computers, is an excellent example of “cyberspace.”

¹¹ It is assumed for pedagogic purposes that the reader is familiar with the commands or languages cited. The appendix has specific examples as well as help listings.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

Electronic Mail

Electronic mail (E-mail) is the network's answer to "telephone tag," the seemingly interminable exchange of "please return my call" messages without direct communications. E-mail allows an individual to consider and reply to each message in his or her own time. It also allows tracking, filing, and other computer aided manipulations. All computer incident handling teams use E-mail to distribute their bulletins and advisories and communicate with each other, and most of the technical community¹².

E-mail is the most popular form of electronic exchange. If a location has any network access at all, it will have E-mail. There are several addressing schemes; we will consider only the popular and common hierarchical Internet form:

`user@localhost.subdomain1...subdomainn.topdomain`

which reads *user* at *localhost* in *subdomain₁* in ... in *subdomain_n* in *topdomain*. For example:

`joe@bigboy.xyzlab.gov`

which is user *joe* on host *bigboy* in subdomain *xyzlab* in the *government* domain. Mail applications vary, but they usually have addressing to individuals or lists, carbon copies, subject field specification, replying, forwarding, and from and date information in the header. They may also have blind carbon copies, binary file attachment, and message ID, received, resent from, and reply to in the header.

The command¹³ to read mail is:

mail [-options]

The command to send mail is:

mail [-options] recipient_list

Help is available by typing ***man mail*** at the command prompt or ***?*** prompt from within mail.

¹² Various groups are addressing issues of confidentiality and integrity; there are interim solutions.

¹³ Commands are assumed to be UNIX unless otherwise specified.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

You may E-mail anonymously through services offered by willing volunteer sites, called “remailers.” One such remailer is located at nowhere@bsu-cs.bsu.edu, and is operated by Chael Hall. (A list of some other sites appears in Appendix I.) It guarantees anonymity and is simple to use. To use this service, make sure that the first two lines of your message contain the following:

first line ::
second line ***Request-Remailing-To: fergp@sytex.com***

Modify any .sig or .mailsig files to suppress signature additions before sending the message. This would reveal your identity.

Anonymous ftp

Anonymous ftp is the network's main library facilitator—either directly, or more recently serving as a partial basis for the reference services. It opens a remarkably cooperative, extremely low cost, timely, ever increasing, and loosely coupled store of valuable and not so valuable information. Not only is there abundant information directly relevant for information technology security specialists, but there is the potential to effectively share greater quantities. For example, all bulletins of the incident response teams, shareware, and freeware¹⁴ are readily available from multiple anonymous ftp sites. It is equally as important for the security specialist to keep abreast of the attacker information also available from anonymous ftp sites. Ironically, some of the sites provide both kinds of information in the spirit of a completely open network.

Anonymous ftp is a special instance of the TCP/IP file transfer protocol, requiring only a user name of “anonymous”—if allowed by the remote site. The password is by convention expected to be your Internet address and user name. Anonymous ftp sites are often library repositories. If the directory is not known beforehand, /pub is usually a good place to start and then you can search down hierarchically.

¹⁴ Shareware is software for which the author requests a nominal fee if the user is satisfied with the product. Freeware is software distributed without cost as a public service.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

To connect to the remote system targ.sub.dom, enter:

ftp targ.sub.dom

At the user name prompt, enter your Internet address. For example:

hero@good.guy.gov

You can now list the top level directory:

ls [-l]

With the -l option, lines that begin with the character “d” will be subdirectories. You can change directories by entering:

cd <directory name>

Print the current working directory:

pwd

Copy a file:

get <file name>

Send a file:

put <file name>

And terminate the session:

quit

Some systems provide introductory or “tidbit” information through the finger command; its format is:

finger @<remote host name>

or

finger <username>@<remote host name>

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

Electronic Bulletin Board Services

Security specialists use electronic bulletin board services (BBSs) as an alternative or in conjunction with E-mail and anonymous ftp. They can “meet” and correspond with other specialists, obtain security bulletins and software, and learn of the latest threats and countermeasures. The CIAC bulletin board service is a good example. See Appendix M for information on CIAC.

Electronic bulletin board services are usually accessed through dial up telephone, data network (such as X.25), or occasionally by Internet. These services tend to be PC oriented and require a suitable terminal emulation package. Workstations and timesharing systems with out-dialing capabilities may also be used. CIAC, National Institute of Standards and Technology (NIST), and the National Computer Security Center (NCSC) through DOCKMASTER provide electronic bulletin board and other services. See Appendix D for further information.

Electronic Conferencing

Electronic conferencing is effectively exploited by the attacker community and other special interest groups. IT security use has been using it to passively learn about new threats. It is an effective means of immediate, value-added communications between physically (and perhaps socially) separate individuals.

Electronic conferencing has been enhanced with the recent development of the Internet Relay Chat (IRC) software. Your local computer (PC, Macintosh, workstation, timesharing system) must obtain the (public domain) software from one of the anonymous ftp sites listed in Appendix E, or from some other source. Assuming you have Internet access, you then connect to one of the listed regional servers—preferably the geographically closest. If your local machine does not have the client software, you can telnet to the site listed in Appendix E to achieve IRC access. Once connected, you may then view and select channels on which to “chat.” To maintain anonymity, use a “handle” rather than your real name if you decide to listen into channel #hack. Also, the server will reveal your Internet location to anyone inquiring—unless you go through the telnet server.

Information flow on IRC tends to be sporadic and frequently flies off on tangents. You can however, initiate a session, invoke recording to disk, and leave it unattended. Other channel participants may notice this, object, and terminate your connections. As a countermeasure, participants have created ‘bots (for robots): script programs designed to appear like a real person listening and making comments. Finally, information may be surreptitiously exchanged between other members of the channel.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

List Servers/ Information Sources

List servers provide the security specialist with timely, topic specific information on narrowly defined subjects. Examples include viruses (Virus-L), means of safely connecting to the network (Firewalls), and the risks of computer and network systems (RISKS digest).

List servers are electronic mailing lists provided to qualified individuals. Moderated lists require that each message be reviewed by a moderator before being resent to the mailing list; on unmoderated lists, all submissions are automatically resent to everyone. Digests are moderated lists that combine all significant messages into periodic mailings. Unless otherwise indicated, you may subscribe to a list by sending an E-mail message to the subscription with the single line:

subscribe listname

in the text portion of the message. The list will then be sent to the address from which you requested the subscription.

Network Information

The Network Information Center (NIC) provides registration information for nodes on the Internet. It is frequently used to find a responsible system administrator for a host that may be attacking a location. Such information includes one or more names, addresses, telephone numbers, and electronic mail addresses.

Network information is provided by the Network Information Center at:

rs.internic.net

You may *telnet* to that address and you will be automatically logged in. The system will show you a help screen and you may then enter commands to get information on users and addresses. The principle command is:

whois domain

or

whois subdomain

You may obtain similar information concerning European hosts by telnetting to:

whois.ripe.net

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

Reference Services

Reference services are emerging as value-added facilities to search through the ever increasing quantities of information available through the Internet. They have the potential to do everything from locating a source of Macintosh anti-viral software to providing the weather report for a city that you're visiting tomorrow.

There are several information servers that allow you to browse the network.

- “**Archie**” is an information locator with which you locate anonymous ftp files. At last count, it could locate 150 gigabytes of information at over 1000 sites. There are a variety of ways to connect, the simplest being where you telnet to one of the server sites listed in appendix H and log in as “archie” (no password is required).
- “**Gopher**” is an Internet resource locator. Its preferred access is through client software on a PC or workstation, but it can be accessed through telnet from a terminal.
- The “**Wide Area Information Server**” (WAIS) is a text retrieval system freely available from Thinking Machines Corporation.
- The “**World Wide Web**” (WWW or W3) provides for the global sharing of academic information. Its source is available through anonymous ftp from CERN. Its growth has exploded in the last year (1994).
- “**Mosaic**” is a rapidly growing, popular “hypermedia” implementation of WWW. According to its creators, it is “an Internet-based global hypermedia browser that allows you to discover, retrieve, and display documents and data from all over the Internet.” It appears to be emerging as a potential de facto standard. Mosaic has the added virtue that it can reference most other services, such as Gopher and ftp (see Appendix H in this document).
- “**Hytelnet**” is a library catalog reference service.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

USEnet News

USEnet news is the interactive news service of the network. The security specialist can selectively read postings on computer security, viruses, privacy issues, attacker methodologies (by the attackers), specific hardware and software, and so on. The specialist can correspond with the authors either privately or through the news service. USEnet is an excellent way of not only learning what's happening, but meeting contemporaries. As with any news source, one should independently verify the information.¹⁵

USEnet news (sometimes referred to as netnews) is selectively accessed through various news reader applications. The news groups are hierarchically defined; some major roots are listed in Appendix J. The news reader application for the purposes this discussion is *m*.

Netnews is a methodology for exchanging information on a common topic. Original articles are "postings" from individuals. Readers may then post replies to postings, replies to replies, and so on. This sequence started by the original posting is called a "thread." News reader applications allow you to "kill" (eliminate) a posting, thread, or news group. Conventionally, if replies contain the text of the referenced posting, it should be indented and/or preceded by a distinguishing character, usually >. Since replies can be nested, one frequently sees postings including various levels of indentation. As a matter of practicality and courtesy, subject lines should be clear and concise.

The "rn" news reader is run by entering: **m**

You will be asked if you want to subscribe to recently added news groups. When that query is finished, you will then be asked to read specific groups. You can answer *yes*, *no*, or *quit*, or you can enter a news group level command. For example, to read the news group "alt.security", type: **g alt.security**

at any point. You will then be shown the chronologically oldest article.¹⁶ Note that all articles have sequential numbers. You can mark the article as read and go on by entering *k*. You can read the next article by entering *n*. You can save an article by typing *s*. You can get a list of all articles by entering *=*. There are other commands that allow you to navigate through a selected news group. You can get help by typing *h*. Note that you must first *quit* reading one news group before you can go to another. Once you are back at the selection level, there are many commands that allow you to navigate through that process. Finally, you can exit completely by typing *q* at the selection level.

¹⁵ Forgeries (known as "spoofing") are possible and do occur occasionally.

¹⁶ If you see a *--more--(x%)* prompt at the bottom of the screen and are unfamiliar with *more* protocol, note the following. Pressing the space bar advances one page and typing *q* quits reading that article. You may also type most other rn commands, for example *n* or *=*.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

The DOE Automated Departmental Directives System (ADDS)

The DOE Automated Departmental Directives System (ADDS) is a database of current DOE and Headquarters Orders, Notices, and Secretary of Energy Notices. It features menu-driven text search and retrieval and reports providing summaries of current and newly issued Directives. The recommended ADDS workstation is an IBM PC (or compatible) with communication software (the FTTERM File Transfer and Terminal Emulator Program is “strongly recommended”), dial out capabilities, a Hayes compatible or BISCAMP modem supporting V.22 or V.32 protocol or DPU in headquarters, and an attached printer. To register, submit DOE forms 1450.5 and 1450.5A to Chief, Human Resource Information Systems, U.S. Department of Energy, AD-123/F-109, Washington, DC 20585. For further information or questions, contact George Hofman at (301) 903-2870.

The National Institute of Standards and Technology (NIST) Electronic Bulletin Board Services

The National Institute of Standards and Technology (NIST) maintains four electronic bulletin board systems for information exchange:

- Computer security
- Data management activities and applications
- Open Systems Interconnections standards activities
- North American Integrated Services Digital Network (ISDN) Users' Forum (NIUF)

The telephone numbers appear in Appendix D of this document.

The DOE Computer Incident Advisory Capability (CIAC) File Server and Electronic Bulletin Board System

The DOE Computer Incident Advisory Capability (CIAC) provides an electronic bulletin board service as well as anonymous ftp. These are in addition to their bulletins and advisories, which are distributed electronically, in hard copy, and (if of immediate importance) by FAX to DOE sites. The BBS and ftp services contain similar information, where the BBS is for those without Internet access. They both feature CIAC and other response team bulletins, virus information, computer security related shareware, utilities, and so on. Access information to these services appears in Appendix M of this document. Use of the BBS is menu driven and self explanatory (note that the current name “CIAC.llnl.gov” will be changing to “ciac.llnl.gov” in the near future). CIAC will be publishing user documentation for both services in the future. If you need further information or help, call the CIAC hotline at (510) 422-8193.

Handling Today's Computer Security Threats— Electronic Resources for Security Related Information, Continued

The National Computer Security Center (NCSC) DOCKMASTER

DOCKMASTER is a (Multics-based) subscription service of the National Computer Security Center (NCSC), that they consider an "Information Security Showcase." Its large repertoire of available services (its users manual is over one hundred pages) includes E-mail, electronic bulletin boards, and allows hands-on software evaluation. Its Evaluated Products List rates computers and computer security products. Users can access online documents (such as the *Orange Book*), participate in online discussions, and learn about computer security conferences. Users can connect to DOCKMASTER through MILNET (part of the Internet), TYMNET (a packet switching service), and local dial-in. A registration packet may be requested by writing to NCSC, Fort George G. Meade, MD 20755-6000—Attn: DOCKMASTER Accounts Administrator. Note that Federal employees are "User Type 3", contractors are "User Type 6" and the project should be "Catwalk" unless you were specifically assigned another one. Further information is available by calling (410) 850-4446—and they are very helpful.

Appendix A

Glossary and Notation

[Note: UNIX commands are case sensitive.]

<u>Term</u>	<u>Description</u>
{ }	alternate choice for the preceding item
[]	containing optional command switches; also, part of file name syntax for some anonymous ftp servers
< >	containing descriptions of fields for commands, such as file names
*	wild card character in file name specification
^	hold down control key while depressing character following the ^
...	recursive wild card directory
anonymous ftp	ftp service not requiring a secret password
archie	internet ftp file locator reference service
bbs	electronic bulletin board system
Betsi	Bellcore's Trusted Software Integrity System
bold type	particularly helpful to attackers/hackers
<i>bold italics</i>	user input in examples; defined terms otherwise
'bots	(from robots) routines to simulate intelligent activity on an irc channel
CIAC	(the DoE) Computer Incident Advisory Capability
.com	commercial organization internet address domain
<cr>	carriage return—typed by user
cracker	term for computer criminal (cf. hacker)
CPSR	Computer Professionals for Social Responsibility
CUD	Computer Underground Digest
cyberspace	the conceptual location of electronic interconnections and communications
CERT	Computer Emergency Response Team
des	Data Encryption Standard
DNS	Domain Name Service—methodology/implementation for routing TCP/IP messages
.edu	educational institution internet address domain
EFF	electronic frontier foundation; organization advocating open information on the internet (among other agenda)
faq	frequently asked questions
FCC	Federal Communications Commission.
(F/C)	telephone number FTS and commercial
finger	UNIX command to obtain user information at a local or remote host
FIRST	Forum of Incident Response and Security Teams
flame	posting critical and sometimes derogatory comments in reply to a posting
freeware	software freely distributed for no cost with owner maintaining all rights
ftp	file transfer protocol; used to send or receive files over the internet
FTS	Federal Telephone System
fyi	for your information

Glossary and Notation, Continued

<u>Term</u>	<u>Description</u>
gif	graphic file format used to exchange pictures
gopher	internet resource locator
.gov	government agency internet address domain
hacker	ambiguous term for computer criminal (original hackers were tinkers in the positive sense; cf. cracker)
handle	electronic pseudonym used for effect and/or to mask identity
HP	Hewlett-Packard
HTML	HyperText Meta Language – “mark up” language for Mosaic hypertext
HTTP	HyperText Transfer Protocol
HYTELNET	Internet library reference service
ICMP	Internet Control Message Protocol
IITF	Information Infrastructure Task Force
<i>italics</i>	defined terms (in text)
irc	internet relay chat; enhanced multi-member electronic conversation
ISDN	integrated services digital network; voice, data, etc., on the same transmission media
ISS	Internet Security Scanner—tool for checking vulnerabilities
IT	Information Technology—blanket term for computer, network, information related activities
kerberos	DES-based encryption scheme—intuitively, a distributed security server
kill	(reading news) eliminate a posting, thread, or newsgroup
mbone	Multicast Backbone—used to broadcast audio and video on the Internet
MD5	message digest algorithm for cryptographic checksums
.mil	military organization internet address domain
MIME	Multipurpose Internet Mail Extensions
mirror	duplication of an ftp distribution site to share distribution overhead
NASIRC	NASA Automated Systems Incident Response Capability
NCSC	National Computer Security Center
.net	backbone networking organization internet address domain
NFS	Network File System
NIC	Network Information Center; assigns/maintains internet addresses
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
.org	non-profit organization internet address domain
OSI	Open Systems Interconnection (networking standards)
PCMCIA	Personal Computer Memory Card International Association
pem	privacy enhanced mail
pgp	pretty good privacy (enhanced mail)
phreaks	attackers who specialize in telephone systems (freaks with a “ph”)
posting	usenet news article
/pub	top level directory usually reserved for public anonymous ftp documents
public domain	software released into the public domain, having no owner or use restrictions
remailer	a site that forwards mail anonymously, removing any identity
rfc	request for comment; technical information notes
ripem	riordan's internet privacy enhanced mail
m	UNIX read news utility
SERT	Security Emergency Response Team (Australia)

Glossary and Notation, Continued

<u>Term</u>	<u>Description</u>
sha	secure hash algorithm
shareware	low cost software, freely distributed with “voluntary” payment requested from satisfied users
sysop	system operator (especially bbs)
.tar	UNIX file name suffix; UNIX archive program format; use <i>tar -fx filename</i> to retrieve
tcp/ip	transport control protocol/internet protocol; networking protocol originally for UNIX and now most other operating systems as well; used for the internet
telnet	remote terminal protocol; used to login to remote hosts on the internet (primarily UNIX)
thread	original posting and all subsequent replies to that posting
TIS	Trusted Information Systems—developers of pem
UNIX	generic term for a number of similar operating systems originally developed by Bell Labs
URL	Uniform (sometimes Universal) Resource Locator: addresses for WWW/Mosaic
.Z	UNIX file name suffix; compressed format for transmission; use <i>uncompress</i> to expand

Appendix B

Anonymous ftp Sites

Format:

internet address:optional directory comments

Log in as **anonymous** password **your username and e-mail address**. Directories usually begin /pub unless otherwise specified. This is not a complete list. You can often find additional information by viewing the parent directories of listed specific subdirectories. Numeric addresses, when available, appear in parentheses.

internet address: **optional directory**

Description/Comment

ames.arc.nasa.gov:pub/SPACE	NASA information, images, etc.
apple.apple.com	Apple/Macintosh
aql.gatech.edu:/pub/eff/cud (128.61.10.53) cud	cud
aql.gatech.edu:/pub/security/iss	security utilities
archive.cis.ohio-state.edu	security software
arisia.xerox.com	message-digest software
arizona.edu	astronomy programs
arthur.cs.purdue.edu:/pub/pcert/tools/unix/netlog-1.02.tar.g	UNIX security tools
arthur.cs.purdue.edu:/pub/reports/TR823.PS.Z	password information
ashley.cs.widener.edu:/pub/src/adm/shadow-3.1.4.tar.Z	password management
aql.gatech.edu	ISS
athena-dist.mit.edu	kerberos software
ba.com	Bell Atlantic
bcm.tmc.edu:/pcnfs/pcnfsd.92.11.05.tar.Z	Sun patches
beach.utmb.edu	anti-virus software backup site
bell.com	telecommunications information
black.ox.ac.uk (129.67.1.165) :/src/security	security information
boombox.micro.umn.edu:/pub/gopher	gopher reference service software
bruno.cs.colorado.edu	?
byrd.mu.wvnet.edu /pub/ejvc/EJVC.INDEX.FTP	Electronic Journal on Virtual Culture
cert.org:/pub/virus-l/docs	virus-l documentation
cert.org:/pub/...	security information (e.g., COPS, npasswd)
coast.cs.purdue.edu	security tools archive
coast.cs.purdue.edu:/pub/aux	security archive
consultant.micro.umn.edu	electronic bookstore
coombs.anu.edu.au:/pub/irc	irc information

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

crl.dec.com:/pub/DEC/ultrix-faq.txt	Ultrix faq
cs.bu.edu:/irc/support	irc
cs.bu.edu:/pub/listserv	list server software
cs.utah.edu:/pub	?
cs.uwp.edu:/pub/msdos/wp/passwp.zip	breaking wordperfect encryption
csn.org	security, etc.
cpsr.org:/cpsr/clinton	white house documents
crvax.sri.com	RISKS digest
csrc.nist.gov:pub/... (129.6.54.11)	NIST bbs, security bulletins, first contacts
cv.vortex.com:/privacy	privacy forum archives
dartvax.dartmouth.edu:/pub/security/passwd+	.tar.Z
dartmouth.edu	password security (UNIX)
decuac.dec.com:/pub/DEC/ultrix-faq.txt	security software
dftnic.gsfc.nasa.gov:[.FILES.MAC]MACSECURE31.HQX{SIT}	Ultrix faq
	anti-virus software
dg-rtp.rtp.dg.com(128.222.1.2)	Data General security patches
dhvx20.csudh.edu:/global_net	global network
drgate.dra.com:/pub/gpo	gpo bbs
ds.internic.net:pub/the-scientist	The Scientist (periodical)
educom.edu	information technology news
eees.nwu.edu	security software
emx.utexas.edu	security software
etext.archive.umich.edu/pub/CuD/cud (141.211.164.18):	cud
eugene.utmb.edu:/pub/pgp	pgp
eugene.utmb.edu:/pub/virus-software/pc{macintosh}	anti-virus software
export.lcs.mit.edu	astronomy programs
faui43.informatik.uni-erlangen.de	irc
fc.net in:/pub/defcon	cracker convention
first.org:/pub	security information
freebie.engin.umich.edu	irc client/server software ftp site
ftp.acsu.buffalo.edu:/pub/irc	irc client/server software ftp site
ftp.alantec.com:pub/tcpr	tcpr software
ftp.apple.com:ds/mac/sys.soft/imaging	apple utilities
ftp.bio.indiana.edu:/util/gopher	gopher software
ftp.bsdi.com	BSDI
ftp.census.gov:/pub	Census bureau
ftp.cert.org:/pub/tools	security tools
ftp.cic.net	internet use instruction
ftp.cisco.com/pub	Cisco (Router/Firewall Vendor)
ftp.cni.org:/CNI/documents/farnet/stories-index	Coaliton for Networked Information Internet
	Information
ftp.ccmil.com	security upgrades
ftp.cco.caltech.edu:/pub/bjmccall	white house documents
ftp.comlab.ox.ac.uk:/pub/Zforum	Z specification language

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

ftp.cs.berkeley.edu:ucb/sendmail	security software
ftp.cs.bul.nl	foreign nodes
ftp.cs.curtin.edu.au:~ftp/pub/netman/[sun4c dec-mips sgi alpha solaris]/[etherman-1.1a interman-1.1 packetman-1.1 loadman-1.0].tar.Z	monitor software
[Also,]~ftp/pub/netman/hershey-[sun4c dec-mips sgi alpha solaris].tar.Z	monitor software
ftp.cs.purdue.edu:/pub/spaf/...	security tools
ftp.cs.purdue.edu:/pub/spaf/COAST/Tripwire	tripwire security software
ftp.cs.ttu.edu:/pub/asciiart	ascii art
ftp.cs.umb.edu:pub/security	security software
ftp.cs.uwm.edu:pub/comp-privacy	computer privacy information
ftp.cs.widener.edu:/pub/zen/...	Zen and the Art of the Internet : A Beginner's Guide to the Internet
ftp.cs.wisc.edu:/connectivity_table	International connectivity table
ftp.cwru.edu:/security/unix-security.ps	unix security
ftp.delmarva.com:pub/security	firewalls information
ftp.denet.dk:pub/misc/tcp	tcp
ftp.denet.dk:/pub/misc/cm200-UFC.tar.Z	password cracker
ftp.digital.com:/pub/Digital/info	Digital Equipment Corporation
ftp.dsi.unimi.it:/pub/security/crypt/worm_src.tar.gz	Internet Worm source code
ftp.ee.mu.oz.au:/pub/text/Cud/...	computer underground digest
ftp.eff.org:/pub/cud/... (192.88.144.4)	computer underground digest, indices, etc.
ftp.eff.org:/pub/irc/lumberjak.shar	irc
ftp.einet.net	gopher sources
ftp.eit.com:/pub/web.guide/	directory of Cyberspace resources
ftp.es.net:/pub/networking-info/earn/nettools.ps{txt}	internet resource guides
ftp.es.net:/pub/security	security information
ftp.etext.org:/Zines/InterText	Intertext electronic periodical
ftp.eunet.no:/pub/text/online.txt	network information—shareware book
ftp.fcc.gov	FCC
ftp.funet.fi:/pub/unix/mail/zmailer/	more secure mailer (than sendmail)
ftp.germany.eu.net:/pub/networking/inet/ethernet/	Ethernet monitors
ftp@ghost.dsi.unimi.it:/pub/crypt/sci.crypt	cryptography
ftp.greatcircle.com:pub/firewalls	firewalls information
FTP.GreatCircle.COM:pub/archive/firewalls.Z	firewalls digest
ftp.gwu.edu:/pub/hoffman	cryptography
ftp.hep.net	High Energy Physics
ftp.inoc.dl.nec.com:pub/security/...(143.101.112.3)	computer security tools
ftp.informatik.uni-hamburg.de:/pub/virus/texts/security	security documents
ftp.informatik.uni-hamburg.de:/pub/virus/texts/tests	virus archives

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

ftp.informatik.uni-hamburg.de:/pub/virus/texts/catalog/msdosvir.zip	ms-dos virus information
ftp.isoc.org/isoc/charts	Internet statistics
ftp.lm.com:pub/interpedia	electronic encyclopedia
ftp.maristb.marist.edu	white house documents
ftp.ncsa.uiuc.edu	NCSA telnet
ftp.ncsa.uiuc.edu:/Mosaic (141.142.20.50)	Mosaic/WWW software
ftp.nec.com:/pub/security/socks/cstc	SOCKS
ftp.netcom.com:/pub/bbosen/Enigma	firewalls
ftp.next.com /pub/NeXTanswers/Files	NeXT patches and security alerts
ftp.netsys.com	computer underground publications
ftp.nisc.sri.com:netinfo/interest-groups	mailing lists, security, etc.
ftp.nisc.sri.com:pub/zone	definitions of internet zones
ftp.ntia.doc.gov	National Information Infrastructure
ftp.oar.net:/pub/OARnet/doc/oarsec.PS.Z	internet security
ftp.ox.ac.uk	cryptography
ftp.pica.army.mil	privacy issues
ftp.pnl.gov in the directory:/pub/pnlinfo	gopher software
ftp.psg.com:pub/unix/netware	security software
ftp.psy.uq.oz.au:/pub/DES	des
ftp.qucis.queensu.ca:pub/dalamb/college-email	how to find e-mail addresses
ftp.rpi.edu	computer mediated communications
ftp.sco.com	SCO UNIX patches
ftp.sei.cmu.edu: /pub/dvk/passwd.ps	password security
ftp.senate.gov	U.S. Senate
ftp.sert.edu.au:/security/sert/tools	tools from Australian SERT
ftp.sgi.com:/pub/sgi/IRIX	SGI patches
ftp.sti.nasa.gov	NASA information
ftp.sura.net:pub/nic	network guides and resources
ftp.tansu.com.au:/pub/docs/security	security documentation
ftp.telebit.com:/pub/nomad/...	network observations
ftp.temple.edu:pub/info/help-net	glossary of computer oriented abbreviations and acronyms
ftp.tidbits.com:/pub/tidbits/issues/	Macintosh information
ftp.tis.com	pem
ftp.tis.com:pub/firewalls	Internet firewall toolkit and papers
ftp.ucsd.edu:hamradio/packet/tcpip/crypto(128.54.16.7)	des source
ftp.unl.edu:/pub/archie/clients	archie client software
ftp.unt.edu:/pub	computer and network security information
ftp.usask.ca:/pub/hytelnet/pc (128.233.3.11)	HYTELNET software
ftp.utdallas.edu:/pub/staff/billy/libguide (129.110.10.1)	internet library guide
ftp.uu.net	dictionaries, astronomy programs
ftp.uu.net:/tmp/CUPindex	cud index
ftp.uu.net:~ftp/systems/sun/sun-dist	sun patches
ftp.win.tue.nl	TCP security tools

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

ftp.win.tue.nl:/pub/security/tcp_wrappers_6.3.shar.Z	TCP wrappers
ftpservers.massey.ac.nz:/pcnfs.sun	sun patches
furmint.nectar.cs.cmu.edu/security	security
garbo.uwasa.fi:/pc/util/wppass2.zip	breaking wordperfect encryption
gatekeeper.dec.com (16.1.0.2)	Third party software for DEC systems
gatekeeper.dec.com:pub/DEC/DECinfo/DECnews-EDU	DECNEWS electronic periodical
gatekeeper.dec.com:/pub/DEC/ultrix-faq.txt	Ultrix faq
gatekeeper.decwrl.com	
gate.demon.co.uk	pgp
ghost.dsi.unimi.it:/pub/crypt	cryptography
ghost.dsi.unimi.it:/pub/security/atp.tar.Z	anti-tampering program, etc.
gopher.uiuc.edu	electronic bookstore
gs80.sp.cs.cmu.edu:/usr/anon/public/space-tech	technical space information
grasp1.univ-lyon1.fr:pub/unix/network/tcpip/security	security software
hafnhaf.micro.umn.edu	"Electronic Government Information Service"
halcyon.com:/pub/mirror/cud/... (202.135.191.2)	mirror of ftp.eff.org
hopf.math.nwu.edu:pub/gn/gn-0.6.tar.Z	gopher software (GN)
ibm1.cc.lehigh.edu	virus-l archives
idlastro.gsfc.nasa.gov	astronomy library
ietf.cnri.reston.va.us:/oc/inet93	INET conference proceedings
iitf.doc.gov	NII
info.umd.edu	Un. of Maryland information/programs
info.umd.edu:/info/Computers/PC/Unix/uuxex520.zip	virus survey
iraun1.ira.uka.de	security, irc
irbis.llnl.gov (128.115.19.60)	CIAC
iris1.ucis.dal.ca:pub/gif	Voyager, Hubble, etc. GIFs
iskut.ucs.ubc.ca:/pub/internet-drafts/draft-rsadsi-rivest-md5-02.txt	MD5 description
jbcondat@attmail.com	Chaos digest - mail server
jerico.usc.edu:pub/gene/kk	cryptographic papers
julius.cs.qub.ac.uk:pub/SpaceDigestArchive	Space Digest
kampi.hut.fi	DES software
kidd.vet.purdue.edu:/pub/users/wam/docs/legal	computer security documents
mac.archive.umich.edu	Macintosh archives
mac.archive.umich.edu:/mac/util/encryption	Macintosh encryption
mcafee.com	antivirus products
mrcnext.cso.uiuc.edu	project Gutenberg online text
mcsun.eu.net	windows security
more@hpcwire.ans.net	technical news stories
naic.nasa.gov:files/general_info/earn-resource-tool-guide.ps,earn-resource-tool-guide.txt	network resources
nasirc.nasa.gov	NASIRC archives

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

net.tamu.edu:pub/security/TAMU	Texas AMU security tools
net-dist.mit.edu:/pub/PGP	PGP
net-dist.mit.edu:/pub/TechMail-PEM	PEM
netlib@research.att.com	compilers
network.ucsd.edu:/intertext (128.54.16.3)	electronic periodical
nevada.edu:/pub/liaison/govrnmnt.zip	Government information on the Internet
nic.funet.fi	network information center, Finland
nic.merit.edu:documents/fyi	network guides and resources
nis.nsf.net:/documents/rfc/...	"requests for comments" standards
nnsf.nsf.net	internet documents
nri.reston.va.us:/ietf	Internet Engineering Task Force
ns.ripe.net:earn /earn-resource-tool-guide.ps,earn-resource-tool-guide.txt	network resource guide
nysernet.org:pub/resources/guides	network guides and resources
oak.oakland.edu	large software repository
oak.oakland.edu:pub/msdos/virus	virus information
ocf.berkeley.edu:/pub/Library/poetry	poetry
otabbs.ota.gov	Office of Technology Assessment (U.S. Federal)
pc10868.pc.cc.cmu.edu	lists
pencil.cs.missouri.edu:/pub/crypt	pretty good privacy (enhanced mail)
photo1.si.edu	Smithsonian photos
pioneer.unm.edu:pub/info/beginner-info	space imagery data
pit-manager.mit.edu:/pub/usenet/...	faq's for the newsgroups
prep.ai.mit.edu	general including fax security
prep.ai.mit.edu:/pub/gnu/fax-3.2.1.tar.Z	net fax software
princeton.edu:/pub/pgp20	pretty good privacy (enhanced mail)
prospero.isi.edu:/pub/papers/security/insurance-cccs94.ps.Z	cryptography
pubinfo.jpl.nasa.gov	JPL
pyrite.rutgers.edu	security mailing list
rascal.ics.utexas.edu:mac/virus-*	anti-virus software
Research.att.com:dist/internet_security	papers on firewalls and breakins
red.css.itd.umich.edu:/cud/...	mirror of ftp.eff.org
rtfm.mit.edu	computer security information
rogue.llnl.gov	DECnet security tools
ripem.msu.edu	ripem programs
ripem.msu.edu:pub/crypt	encryption software
risc.ua.edu:/pub/ibm-antivirus	anti-virus software
rpub.cl.msu.edu	RSAREF
rsa.com:/pub/...	cryptography
rsa.com:/rsaref/dist/930105	RIPEM, RSAREF
rtfm.mit.edu:/pub/usenet	usenet faq archive
rutgers.edu	Columbia University Appletalk
s1.gov	security software
s1.gov:/pub/socks.tar.Z	UNIX security
s6k.boulder.ibm.com	IBM security fixes
sc.tamu.edu:pub/security/TAMU	network security tools
sipb.mit.edu:/pub/diswww/diswww.tar.gz	electronic conferencing source (Discuss)

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

slopoke.mlb.semi.harris.com:/pub/irc	irc client/server software ftp site
soda.berkeley.edu:/pub/cyberpunks	remailer usage
soda.berkeley.edu:/pub/cyberpunks/pgp	pgp
software.watson.ibm.com	IBM fixes
solbourne.solbourne.com	Solbourne information (including security fixes)
src.doc.ic.ac.uk:/computing/comms/irc	irc information
src.doc.ic.ac.uk:/public/sun/pc-nfs/pcnfsd.92.11.05.tar.Z	Sun patches
src-aux.src.umd.edu	Macintosh information/software
sumex-aim.stanford.edu	Apple software
sumex-aim.stanford.edu:/info-mac/virus	anti-virus software
sunsite.unc.edu	linux fixes
sunsite.unc.edu:/home3/wais/white-house-papers	white house documents
sunsolve1.sun.com:/pub/patches	SUN patches
suburbia.apana.org.au:/pub/proff/worm	Internet Worm source code
techreports.larc.nasa.gov:pub/techreports/larc/92	NASA technical reports
thumper.bellcore.com:/pub/skey	s/key one time password software
thumper.bellcore.com:/pub/crypt	cryptography
Town.Hall.Org	Edgar—Securities and Exchange information
uiunix.ui.org	UNIX standards
una.hh.lib.umich.edu:/inetdirsstacks	internet resource guides
unma.unm.edu	ethics, policy, legislation
urvax.urich.edu:[MSDOS.ANTIVIRUS]/info-mac/virusux1.cso.uiuc.edu:/pc/virus	anti-virus software
ucsd.edu:/hamradio/packet/tcpip/crypto/des.tar.Z	DES code
uunet.uu.net:comp.sources.misc/volume23/smiley/part01.Z	smiley sources
venera.isi.edu	DNS tools
vitruvius.cecer.army.mil	binary gifs
van-bc.wimsey.bc.ca:/pub/crypto/PGP-2.1	pgp
world.std.com:/OBS/The.Internet.Companion/	internet documentation
wsmr-simtel20.army.mil	large software repository
wsmr-simtel20.army.mil:PD1:<MSDOS.TROJAN-PRO>{PD3:<MACINTOSH.VIRUS>}	anti-virus software
wuarchive.wustl.edu	largest software repository
wuarchive.wustl.edu.: /doc/misc/*	documentation
wuarchive.wustl.edu:ftp/usenet/comp.virus/*	unix security
wuarchive.wustl.edu:usenet/comp.sources.misc/volume23/smiley/part01.Z	smiley sources
yuma.acns.colostate.edu:/software.ibmpc/beholder/beholder.zip	Monitor software

Appendix C

Finger Sources

These are usually electronic “tidbits” you may obtain by typing:

finger <sourcename>

For example, to obtain local Livermore, CA weather, type:

finger weather@icaen.llnl.gov

Appendix D

BBSs

BBS

Access Methods

cc:Mail BBS	(415) 691-0401
CIAC	(510) 423-4573 (1200/2400 baud); (510) 423-3331 (9600 baud)
U.S. Commerce Department Internet access	(202) 482-3870 (2400 baud); (202) 482-2167 (9600 baud) Telnet to "ebb.stat-usa"
Fedworld BBS, access to federal information services, versatile, complex	(703) 321-8020 (sys op (703) 487-4608))
IITF bulletin board	(202) 501-1920
Backup	(202) 482-1199
Internet access	Telnet to "iitf.doc.gov" and log in as <i>gopher</i>
Questions	(202) 482-1835; E-mail cfranz@ntia.doc.gov
NIST computer security	(301) 948-5717 (2400 baud or less); (301) 948-5140 (9600 baud)
Internet access	Telnet to "cs-bbs.ncsl.nist.gov" (129.6.54.30)
NIST data management activities and applications	(301) 948-2048 or (301) 948-2059 (2400 baud or less)
NIST open systems interconnection standards	(301) 869-8630 (2400 baud or less)
NIST North American Integrated Services Digital Network User's Forum	(301) 869-7281 (2400 baud or less)
The Privacy Rights Clearinghouse BBS	Direct access: (619) 260-4670 At the local prompt enter <i>c teetot</i> At the login prompt enter <i>privacy</i> Follow instructions for new users
Internet access	Telnet to "teetot.acusd.edu" and follow the above steps

Read the USEnet newsgroup "alt.bbs" for information about bulletin board services.

Appendix E

IRC (Internet Relay Chat) Conferencing

<u>Location</u>	<u>Description</u>
#hack	attacker channel (there are many other channels, most legitimate)
bradenville.andrew.cmu.edu	telnet server
cc.nsysu.edu.tw	telnet server - login: irc
chatsubo.nerce.gov:login bbs	telnet server
ircserver.itc.univie.ac.at 6668	telnet server
irc.ibmpcug.co.uk 9999	telnet server
irc.santafe.edu	telnet server - login: irc
cs.bu.edu:/irc/clients	irc client/server software ftp site
ftp.acsu.buffalo.edu:/pub/irc	irc client/server software ftp site
freebie.engin.umich.edu	irc client/server software ftp site
slopoke.mlb.semi.harris.com:/pub/irc	irc client/server software ftp site
(US)badger.ugcs.caltech.edu	irc server site (US)
csd.bu.edu	irc server site (East Coast US)
disuns2.epfl.ch	irc server site (Switzerland)
irc.caltech.edu	irc server site (Westcoast US)
munagin.ee.mu.oz.au	irc server site (Australia)
nic.funet.fi	irc server site (Finland)
penfold.ece.uiuc.edu	irc server site (Midwest US)

IRC (Internet Relay Chat) Conferencing, Continued

<code>sunsystem2.informatik.tu-muenchen.de</code>	irc server site (Germany)
<code>ucsu.colorado.edu</code>	irc server site (US)
<code>ug.cs.dal.ca</code>	irc server site (Canada)

Appendix F

List Servers/Information Sources

<u>List Server/Source</u>	<u>Description</u>
bugtraq-request@fc.net cert@cert.org cert@cert.org ciac-listproc@llnl.gov ciac-listproc@llnl.gov comp-privacy-request@pica.army.mil gopher-news-request@boombox.micro.umn.edu interpedia-request@telerama.lm.com isoc@nri.reston.va.us listproc@educom.edu listserv@itocsivm.csi.it	bugtraq cert-advisories cert-tools ciac-bulletin CIAC-notes computer privacy digest subscription gopher news subscription Interpedia on-line encyclopedia Internet Society News EDUCOM information technology news Network Information Retrieval and Online Public Access Catalogs
LISTSERV@KENTVM.BITNET LISTSERV@LEHIGH.EDU LISTSERV@LEHIGH.EDU listserv@vmd.cso.uiuc.edu mac-security-request@eclectic.com Majordomo@GreatCircle.COM majordomo@is.internic.net Majordomo@Lists.EUnet.fi Majordomo@net.tamu.edu majordomo@nsmx.rutgers.edu pem-dev-request@tis.com pem-info@tis.com phrack@well.sf.ca.us privacy-request@cv.vortex.com risks-request@csl.sri.com security-alert@flatline.corp.sun.com security-features@sun.com tk0jut2@mvs.cso.niu.edu dds.hacktic.nl	HYTEL-L list sever (internet library guide) ms-dos viruses; SUB VIRUS-L yourfullname ms-dos viruses alert; SUB VALERT-L yourfullname CUD, SUB CUDIGEST YOUR NAME Macintosh security subscription firewalls and firewalls-digest subscription scout-report, weekly happenings cryptography; SUBSCRIBE CYPHERWONKS academic-firewalls www-security pem subscription privacy enhanced mail information Phrack periodical privacy forum digest subscription risks digest subscription Sun security information Sun security alerts Computer Underground Digest (telnet) The Digital City

Appendix G

Network Information

Telnet to “rs.internic.net”. The primary command is:

whois domain

or

whois subdomain

Appendix H

Reference Services

Archie

Archie is used for automated anonymous ftp server searches (see anonymous ftp for client software). There are multiple file locator sites (telnet to site and log in as *archie*):

archie.rutgers.edu (Rutgers University)
archie.unl.edu (University of Nebraska in Lincoln)
archie.sura.net (SURAnet archie server)
archie.ans.net (ANS archie server)

Gopher (Internet Resource Server)

- **Client software:**

boombox.micro.umn.edu:/pub/gopher
ftp.bio.indiana.edu:/util/gopher

- **Telnet access:**

consultant.micro.umn.edu (134.84.132.4)
gopher.uiuc.edu (128.174.33.160)
panda.uiowa.edu (128.255.40.201)

- **Servers:**

ace.esusda.gov – Americans Communicating Electronically (Department of Agriculture)
aclu.org – ACLU
ba.com – Bell Atlantic
bell.com – telecommunications information
csbh.com – Computer Solutions by Hawkinson
cix.org – commercial information
cwis.usc.edu – Gopher Jewels
dewey.lib.ncsu.edu – North Carolina State University Library
ds.internic.net – InterNIC network information service
educom.edu – EDUCOM Documents and News
fatty.law.cornell.edu – Cornell Law School
fedix.fie.com – Federal Info. Exchange (FEDIX)
gopher.acusd.edu – Privacy Rights Clearinghouse
gopher.bcm.tmc.edu – Baylor College of Medicine
gopher.census.gov – Census bureau
gopher.cic.net – internet use instruction

Reference Services, Continued

gopher.cic.net:Electronic Serials/Alphabetic List/e/Electronic Journal on Virtual Culture/ – Electronic Journal on Virtual Culture
gopher.cni.org:70/11/cniftp/miscdocs/farnet – Coalition for Networked Information Internet Information
gopher.cpsr.org – CSPR
gopher.cs.ttu.edu – Texas Tech University
gopher.decus.org – DECUS
gopher.ed.gov – Department of Education
gopher.eff.org – EFF
gopher.epa.gov – EPA
gopher.es.net – Energy Sciences network
gopher.esa.doc.gov – U.S. Commerce Department
gopher.fcc.gov – FCC
gopher.first.org – FIRST
gopher.fonorola.net – Internet Business Journal archives
gopher.gsfc.nasa.gov – NASA Goddard Space Flight Center
gopher.house.gov – U.S. House of Representatives
gopher.internet.com – Electronic Newsstand information
gopher.lanl.gov – Los Alamos National Laboratory
gopher.law.csuohio.edu – Cleveland State University Law Library
gopher.lib.umich.edu – University of Michigan Libraries, Internet Resource Guides
gopher.nara.gov – National Archives
gopher.netsys.com (port 2100) – Electronic Newsstand (problems e-mail to staff@enews.com)
gopher.nist.gov – National Institute of Standards and Technology
gopher.ox.ac.uk:The World/Gopherspace/Alex – electronic texts
gopher.senate.gov – U.S. Senate
gopher-server.nist.gov – National Institute of Standards and Technology (NIST)
gopher.sti.nasa.gov
gopher.tamu.edu – Texas A&M
gopher.tic.com – EFF-Austin/IMatrix Information and Directory Services, Inc. (MIDS), Austin
gopher.town.hall.org – Internet radio
gopher.undp.org – United Nations
gopher.unr.edu – University of Nevada
gopher.vortex.com – Vortex Technology
gopher.well.sf.ca.us – Whole Earth 'Lectronic Magazine - The WELL's Gopherspace
gopher.wired.com – public cryptography issues
hopf.math.nwu.edu – Internet Society, gopher software
ici.proper.com – Internet Computer Index
ietf.CNRI.Reston.Va.US
iitf.doc.gov – information infrastructure
info.asu.edu – electronic periodicals and educational gopher sites
info.learned.co.uk – LI NewsWire electronic periodical
internic.net – Network Information Center Gopher
jupiter.esd.ornl.gov – Oak Ridge National Laboratory ESD Gopher
krakatoa.jsc.nasa.gov – Library X at Johnson Space Center
lawnext.uchicago.edu – University of Chicago Law School

Reference Services, Continued

liberty.uc.wlu.edu – Washington & Lee University (Legal)
marketplace.com – Internet information mall
marvel.loc.gov – Library of Congress (LC MARVEL)
naic.nasa.gov – NASA Network Applications and Information Center
(NAIC)
ns.novell.com – Novell Netwire Archives
nsth.nu.ca – electronic bookstore
ntiaunix1.ntia.doc.gov – National Information Infrastructure
ocs.dir.texas.gov – Department of Information Resources (State of Texas)
pdb.pdb.bnl.gov – Brookhaven National Laboratory Protein Data Bank
rs.internic.net – NIC
sluava.slu.edu – Saint Louis University (Legal)
SunSITE.unc.edu (152.2.22.81) – SUN information
technology.com – NASA Mid-Continent Technology Transfer Center
tic.com – Texas Internet Consulting
trainmat.ncl.ac.uk – network training
twinbrook.cis.uab.edu – Interpedia project
ucsbuxa.ucsb.edu (port 3001) – University of California - Santa Barbara
Library
una.hh.lib.umich.edu – University of Michigan internet resource guides
vienna.hh.lib.umich.edu
vx740.gsfc.nasa.gov – NASA Shuttle Small Payloads Info
wired.com – writing
wiretap.spies.com – Wiretap
world.std.com – The World (Public Access UNIX)

Wide Area Information Server

brewster@think.com – E-mail for further information
quake.think.com – telnet and sign on as “wais”
wais.eff.org – EFF

World Wide Web/Mosaic

- **Client software:**

info.cern.ch/pub/www/WWWLineModeDefaults.tar.Z - browser source
ftp.ncsa.uiuc.edu (141.142.20.50) – Mosaic

- **Servers (Uniform Resource Locators):**

You may access any anonymous ftp server xxx.yyy.zzz as ftp://xxx.yyy.zzz and any gopher server with the prefix gopher:// as illustrated below. The slashes (/) following the reference address delineate directory, subdirectory, ..., file name in the usual Unix notation.

ftp://ftp.tidbits.com/pub/tidbits/issues/ – Macintosh information
gopher://aclu.org:6601/1 – ACLU
gopher://arl.cni.org:70/11/scomm/edir – directory of electronic journals
gopher://ba.com – Bell Atlantic
gopher://ds.internic.net/1/pub/niclocator – network information center
gopher://gopher.es.net/11/pub/security – Energy Sciences network

Reference Services, Continued

[gopher://gopher.es.net/11/pub/ota](http://gopher.es.net/11/pub/ota) – security documentation
[gopher://ntiaunix1.ntia.doc.gov:70/11s/newitems](http://ntiaunix1.ntia.doc.gov:70/11s/newitems) – National Information Infrastructure
gopher://oss968.ssa.gov – Social Security Administration
gopher://peg.cwis.uci.edu:7000/11/gopher.welcome/peg/GOPHERS/gov – U.S. Government
gopher://rsl.ox.ac.uk:70/11/lib-corn/hunter – electronic texts
gopher://UMSLVMA.UMSL.EDU:70/11/LIBRARY/GOVDOCS/WF93 – CIAC World Fact Book (University of Missouri server)
gopher://una.hh.lib.umich.edu/11/inetdirs – University of Michigan
<http://akebono.stanford.edu/yahoo/> – Resource locator
<http://aps.org/> – American Physical Society
<http://att.net/dir800> – 800 number directory
<http://core.symnet.net/~VOU/> – Virtual Online University
<http://csrc.ncsl.nist.gov/> – FIRST
<http://curia.ucc.ie/info/net/acronyms/acro.html> – Acronym translator
<http://delcano.mit.edu/> – NASA planetary data
<http://delcano.mit.edu/cgi-bin/midr-query> – NASA planetary data
<http://dfw.net/~aleph1> – cracker home page
<http://digicash.support.nl/> – digital cash
<http://ds.internic.net/ds/dsdirofdirs.html> – InterNIC network information center
<http://educom.edu/.index.html> – Educom
<http://first.org> – FIRST
<http://ftp.etext.org/Zines/InterText/intertext.html> – electronic periodical
<http://freeside.com/phrack.html> – phrack home page
<http://http2.sils.umich.edu/~lou/chhome.html> or <http://http2.sils.umich.edu/~lou/chhome.html> – University of Michigan
<http://ici.proper.com> – Internet Computer Index
<http://info.acm.org/> – ACM
<http://info.bellcore.com/BETSI/betsi.html> – Betsi
<http://info.cern.ch/hypertext/DataSources/bySubject/Overview.html> – WWW virtual library
<http://info.cern.ch/wit> – WIT WWW conversation software
<http://info.cern.ch/hypertext/WWW/Clients.htm> – browser programs
<http://info.cern.ch/hypertext/WWW/FAQ/Bootstrap.html> – telnet accessible browsers
<http://info.cern.ch/hypertext/WWW/Shen/ref/shen.html> – Mosaic security
<http://info.isoc.org/interop-tokyo.html> – Internet information
<http://info.learned.co.uk> – LI NewsWire electronic periodical
<http://jupiter.esd.ornl.gov/> – Oak Ridge National Laboratory ESD
<http://lcweb.loc.gov/homepage/lchp.html> – Library of Congress
[http://login.eunet.no/\(presno/](http://login.eunet.no/(presno/) – Online World resources handbook
<http://marketplace.com> – Internet information mall
<http://nearnnet.gnn.com/GNNhome.html> – Global Network Navigator
<http://pass.wayne.edu/business.html> – business on the Internet
<http://peterhe.ulib.albany.edu/mk-docs/mk-isp.html> – list of libraries
<http://power.globalnews.com/> – PowerPC News
<http://programs.interop.com>
<http://pubweb.parc.xerox.com/map> – Xerox PARC Map Viewer
<http://pubweb.ucdavis.edu/Documents/Quotations/homepage.html> – quotations

Reference Services, Continued

http://stardust.jpl.nasa.gov/pds_home.html – NASA planetary data
<http://sunsite.unc.edu/ianc/index.html> – “Underground music”
<http://uu-gna.mit.edu:8001/uu-gna/text/index.html> – texts for on line classes
<http://web.nexor.co.uk/mak/doc/robots/robots.html> – WWW robots
<http://wombat.doc.ic.ac.uk/> – On-line Dictionary of Computing
<http://www-ns.rutgers.edu/www-security/index.html> – WWW security
<http://www.anl.gov/oithome.html> – Department of Energy
<http://www.ba.com> – Bell Atlantic
<http://www.border.com/> – firewall vendor
<http://www.brandonu.ca/~ennsnr/Resources/resources.html> – Internet training resources
<http://www.census.gov/> – Census bureau
<http://www.cis.ohio-state.edu/hypertext/faq/usenet/FAQ-list.html> – USEnet faqs
<http://www.charm.net/~web/Vlib.html> – WWW page development
<http://www.clark.net/pub/listserv/listserv.html> – listserv lists
http://www.commerce.net/directories/members/ns/new_ipower.html – National Semiconductor security products
http://www.cs.colorado.edu/homes/mcbryan/public_html/bb/summary.html – World-Wide WAIS-Searchable WWW Catalogues
<http://www.decus.org/> – DECUS
<http://www.di.unipi.it/iconbrowser/icons.html> – Icon Browser at Pisa University
<http://www.digital.com/home.html> – Digital Equipment Corporation
<http://www.earn.net/lug/notice.html> – list servers
<http://www.ed.gov/> – Department of Education
<http://educom.edu/> – EDUPAGE
<http://www.ee.surrey.ac.uk/edupage/edupage/> – Edupage electronic periodical
http://www.eecs.nwu.edu/hacker_crackdown/index.html – “The Hacker Crackdown”
<http://www.eff.org/ftp/EFF> – EFF
<http://www.eit.com/web/www.guide/> – guide to Cyberspace
<http://www.ensta.fr/internet/> – Internet “goodies”
<http://www.es.net/pub/ota> – security documentation
<http://www.fcc.gov> – FCC
<http://www.fedworld.gov> – U.S. Government servers
<http://www.Four11.com> – e-mail directory service
<http://www.geom.umn.edu/docs/snell/chance/welcome.html> – probability and statistics
<http://www.hp.com> – HP Main Welcome Screen
<http://www.hpcc.gov/imp95/> – High Performance Computing and Communications
<http://www.hull.ac.uk/Hull/ITTI/itti.html> – United Kingdom's Information Technology Training Initiative
<http://www.ictp.trieste.it/Canessa/whoiswho.html> – Who's Who on the Internet
<http://www.ihep.ac.cn:3000/china.html> – Peoples Republic of China
<http://www.info.apple.com/> – Apple
<http://www.internic.net/> – the interNIC

Reference Services, Continued

<http://www.internic.net/infoguide.html> – guide to Internet WWW resources
<http://www.jou.ufl.edu/commres/webjou.html> – links to newspapers
<http://www.kiae.su/www/wtr/> – Window-to-Russia
<http://www.lib.umich.edu/chhome.html> or – University of Michigan
<http://www.lib.virginia.edu/etext/ETC.html> – University of Virginia
<http://www.llnl.gov> – Lawrence Livermore National Laboratory
<http://www.media.org/> – MIT security products
<http://www.mit.edu:8008/> – electronic conferencing (Discuss)
<http://www.nara.gov> – National Archives
<http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/Docs/whats-new.html> – new server announcements
<http://www.netmarket.com/> – encrypted Mosaic
<http://www.nw.com> – Internet statistics
<http://www.openmarket.com/info/internet-index/current.html> Internet tidbits
<http://www.ora.com/cgi-bin/ora/currency> – currency exchange rates
<http://www.ornl.gov/> – Oak Ridge National Laboratory
<http://www.research.att.com/> – ATT Bell Labs
<http://www.rpi.edu/~decemj/cmc/mag/current/toc.html> – Computer-Mediated Communication Magazine
<http://www.rpi.edu/Internet/Guides/decemj/text.html> – Internet resources
<http://www.scubed.com:8001/> – IRS and state tax forms
<http://www.sei.cmu.edu/FrontDoor.html> – Software Engineering Institute
<http://www.service.com/PAW/home.html> – Palo Alto Weekly
http://www.ssa.gov/SSA_Home.html – Social Security Administration
<http://www.tansu.com.au/Info/security.html> – security information
<http://www.tansu.com.au/hypermil/index.html> – mailing list archives
<http://www.tis.com/> – Trusted Information Systems
<http://www.town.hall.org/> – Internet radio
<http://www.tu-graz.ac.at/CHCIbib> – Human Computer Interaction
<http://www.utirc.utoronto.ca:3232/HTMLdocs/NewHTML/intro.html> – HTML documentation
<http://www.vortex.com/> privacy information
<http://www.wais.com> – Wide Area Information Server
<http://www.wais.com/wais-dbs/risks-digest.html> – risks digest
<http://www.whitehouse.gov> – White House
<http://www.willamette.edu/~tjones/Spanish> – Spanish lessons
<http://www.wired.com> – public cryptography issues
<http://www.wsg.hp.com/> – HP Workstation Systems Group
<http://www.whoost.cc.utexas.edu/world/instruction/index.html> – instructional uses of the web
<http://130.20.92.130:8001/esh/home2.htm> – DOE Office of Environment, Safety and Health

Appendix I

Remailers

Edited List

- 1 hh@pmantis.berkeley.edu
- 2 hh@cicada.berkeley.edu
- 3 hh@soda.berkeley.edu
- 4 nowhere@bsu-cs.bsu.edu
- 5 remail@tamsun.tamu.edu
- 6 remail@tamaix.tamu.edu
- 7 ebrandt@jarthur.claremont.edu
- 8 hal@alumni.caltech.edu
- 9 remailer@rebma.mn.org
- 10 elee7h5@rosebud.ee.uh.edu
- 11 phantom@mead.u.washington.edu
- 12 hfinney@shell.portal.com
- 13 remailer@utter.dis.org
- 14 00x@uclink.berkeley.edu
- 15 remail@extropia.wimsey.com

Notes:

- 1 through 6: do not support encrypted headers.
- 7 through 12: support encrypted headers.
- 9, 13, 15: introduce longer than average delay; privately owned machines.
- 14: public key not yet released.
- 15: header and message must be encrypted together.

Others

admin@anon.penet.fi

Appendix J

USEnet News

Relevant Major Roots	alt	alternative, testing
	comp	computer related
	gnu	software from Free Software Foundation
	ieee	IEEE related
	misc	miscellaneous
	sci	science
	talk	discussion of specific topic
	vmsnet	VMS related

Relevant Groups	austin.eff
	alt.2600
	alt.bbs.lists
	alt.irc
	alt.privacy
	alt.security
	alt.security.index
	alt.security.pgp
	bit.listserv.infonets
	bit.listserv.virus-l
	comp.infosystems.gopher
	comp.org.eff.talk
	comp.risks
	comp.security.announce
	comp.security.misc
	comp.society.cu-digest
	comp.society.privacy
	comp.sources.binaries
	comp.sys.novell
	comp.virus
	misc.security
	sci.crypt
	sci.virus

Appendix K

FIRST

Since November of 1988, an almost continuous stream of security-related incidents has affected thousands of computer systems and networks throughout the world. To address this threat, a growing number of government and private sector organizations around the globe have established a coalition to exchange information and coordinate response activities. This coalition, the Forum of Incident Response and Security Teams (FIRST), brings together a variety of computer security incident response teams from government, commercial, and academic organizations. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large. Currently, FIRST has more than 30 members.

You can learn more about FIRST and obtain a list of member incident response teams through the FIRST WWW at [http://first.org/first/#What's FIRST](http://first.org/first/#What's%20FIRST).

Appendix L

References

Cronin, Mary J., *Doing Business on the Internet*, Van Nostrand Reinhold, 1994.

Fraase, Michael, *The MAC Internet Tour Guide*, Ventana Press, 1993.

Frey, Donnalyn & Adams, Rick, *!%@:: A Directory of Electronic Mail Addressing and Networks*, O'Reilly & Associates, Inc., 1990.

Krol, Ed, *The Whole Internet User's Guide and Catalog*, O'Reilly & Associates, Inc., 1992.

LaQuey, Tracy, with Ryer, Jeanne C., *The Internet Companion—A Beginner's Guide to Global Networking*, Addison Wesley, 1993

Marine, April, editor, *Internet: Getting Started*, SRI International, 1992.

Network Information Center, *DDN NEW USER GUIDE*, anonymous FTP from
nic.ddn.mil:netinfo/nug.doc.

Quarterman, John S., *The Matrix: Computer Networks and Conferencing Systems Worldwide*, Digital Press, 1990.

Appendix M

Contacting CIAC

Phone	(510) 422-8193
Fax	(510) 423-8002
STU-III	(510) 423-2604
Electronic mail	ciac.llnl.gov
Emergency SKYPAGE	800-SKYPAGE pin# 855-0070
Anonymous FTP server	ciac.llnl.gov (IP 128.115.19.53)
BBS	(510) 423-3331 (9600 Baud) (510) 423-4753 (2400 Baud)

Reader Comments

CIAC updates and enhances the documentation it produces. If you find errors in or have suggestions to improve this document, please fill out this form. Mail it to CIAC, Lawrence Livermore National Laboratory, P.O. Box 808, Mail Stop L-303, Livermore, CA, 94551-9900. Thank you.

List errors you find here. Please include page numbers.

List suggestions for improvement here.

Optional:

Name _____ Phone _____

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551